



Venner Shipley
200 Aldersgate
London EC1A 4HD
United Kingdom

T +44 (0)20 7600 4212
F +44 (0)20 7600 4188
mail@vennershipley.co.uk

www.vennershipley.co.uk

The European Patent Office
D-80298 München
Germany

By epoline

19 June 2017

Dear Sirs,

European Patent Application No. 15722292.8

Centripetal Networks, Inc.

Our ref: PSD/JRV/81546EP1

We write in response to the R161 Communication (the Communication) dated 7 December 2016, and address the alleged deficiencies raised in the Written Opinion of the ISA.

Amendments

We file herewith amended claims 1-15, in both clean and annotated versions.

Original claims 1-9 and 19-20 have been deleted.

New claims 10-15 have been provided. Basis for these claims can be found as follows:

Claim	Basis
10	Paragraph [51]
11	Paragraphs [45], [53] and [86]
12	Paragraphs [0044]-[0046], [0068]-[0070], [0081]-[0083] and [86]

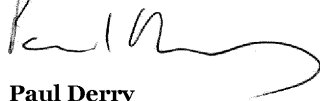
19 June 2017
Page 2

13	Paragraphs [0044], [0046], [0068]-[0070], [0082]-[0083] and [0087]
14	Paragraphs [0090] and [0091]
15	Paragraphs [0090] and [0091]

The remaining original claims and their dependencies have been renumbered accordingly. Multiple dependencies have been included, basis for which can be found throughout the specification.

These claims were not searched in the international phase. An additional search fee is paid herewith.

Yours faithfully,



Paul Derry
Authorised Representative

Enc. Amended claims 1-15 (clean and annotated versions)
Search fee

Claims

- ~~401.~~ A method, comprising:
- receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that includes at least one rule specifying packet-identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria;
 - receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;
 - identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria; and
 - performing, by the packet security gateway and on a packet-by-packet basis, the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria.
- ~~442.~~ The method of claim ~~10~~, wherein performing the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria comprises:
- identifying a subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and
 - generating, for each of the one or more packets corresponding to the packet-identification criteria, a record comprising the subset of information specified by the packet digest logging function.
- ~~423.~~ The method of claim ~~24~~, wherein the subset of information comprises at least one of a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the

packet security gateway that received the packet, or one or more media access control (MAC) addresses associated with the packet.

- | ~~434.~~ The method of claim ~~442~~, comprising:
 - temporarily storing data in a memory of the packet security gateway, the data comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and
 - utilizing, by the packet security gateway, the data to generate a message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria.
- | ~~445.~~ The method of claim ~~434~~ comprising communicating, by the packet security gateway and to the security policy management server, the message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria.
- | ~~456.~~ The method of claim ~~442~~, comprising reformatting, for each of the one or more packets corresponding to the packet-identification criteria, the subset of information specified by the packet digest logging function in accordance with a logging system standard.
- | ~~467.~~ The method of claim ~~456~~, wherein reformatting the subset of information specified by the packet digest logging function in accordance with the logging system standard comprises reformatting the subset of information specified by the packet digest logging function in accordance with a syslog logging system standard.
- | ~~478.~~ The method of claim 10, wherein the packet-identification criteria comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria corresponds to at least one of the one or

more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports.

489. The method of claim 10, wherein the packet-identification criteria comprises application-layer packet-header information, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria comprises at least a portion of the application-layer packet-header information.

10. The method of claim 1, wherein the packet-identification criteria comprise a Differentiated Service Code Point, DSCP, descriptor.

11. The method of claim 1, further comprising:
routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function.

12. The method of claim 1, wherein the packet transformation function comprises an accept packet transformation function; and

wherein the performing the packet digest logging function comprises:
forwarding, by the packet security gateway, the each of the one or more packets corresponding to the packet identification criteria toward its respective destination.

13. The method of claim 1, wherein the packet transformation function comprises an deny packet transformation function; and

wherein the performing the packet digest logging function comprises:
dropping, by the packet security gateway, the each of the one or more packets corresponding to the packet identification criteria.

14. A system comprising at least one processor and a memory storing instructions that, when executed by the at least one processor, cause the system to perform one or more of the methods of claims 1 to 13.

15. A computer program comprising computer-executable instructions that, when executed by one or more processors, cause the one or more processors to perform one or more of the methods of claim 1-13.

Claims

1. A method, comprising:
 - receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that includes at least one rule specifying packet-identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria;
 - receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;
 - identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria; and
 - performing, by the packet security gateway and on a packet-by-packet basis, the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria.
2. The method of claim 1, wherein performing the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria comprises:
 - identifying a subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and
 - generating, for each of the one or more packets corresponding to the packet-identification criteria, a record comprising the subset of information specified by the packet digest logging function.
3. The method of claim 2, wherein the subset of information comprises at least one of a portion of data from the packet, a source address of the packet, a source port of the packet, a destination address of the packet, a destination port of the packet, a transport-protocol type of the packet, a uniform resource identifier (URI) from the packet, an arrival time of the packet, a size of the packet, a flow direction of the packet, an identifier of an interface of the

packet security gateway that received the packet, or one or more media access control (MAC) addresses associated with the packet.

4. The method of claim 2, comprising:
 - temporarily storing data in a memory of the packet security gateway, the data comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria; and
 - utilizing, by the packet security gateway, the data to generate a message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria.
5. The method of claim 4 comprising communicating, by the packet security gateway and to the security policy management server, the message comprising the subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria.
6. The method of claim 2, comprising reformatting, for each of the one or more packets corresponding to the packet-identification criteria, the subset of information specified by the packet digest logging function in accordance with a logging system standard.
7. The method of claim 6, wherein reformatting the subset of information specified by the packet digest logging function in accordance with the logging system standard comprises reformatting the subset of information specified by the packet digest logging function in accordance with a syslog logging system standard.
8. The method of claim 1, wherein the packet-identification criteria comprises a five-tuple specifying one or more transport-layer protocols, a range of source addresses, a range of source ports, a range of destination addresses, and a range of destination ports, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria corresponds to at least one of the one or

more transport-layer protocols, has a source address within the range of source addresses, a source port within the range of source ports, a destination address within the range of destination addresses, and a destination port within the range of destination ports.

9. The method of claim 1, wherein the packet-identification criteria comprises application-layer packet-header information, and wherein identifying the one or more packets corresponding to the packet-identification criteria comprises determining by the packet security gateway that each of the one or more packets corresponding to the packet-identification criteria comprises at least a portion of the application-layer packet-header information.
10. The method of claim 1, wherein the packet-identification criteria comprise a Differentiated Service Code Point, DSCP, descriptor.
11. The method of claim 1, further comprising:
routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function.
12. The method of claim 1, wherein the packet transformation function comprises an accept packet transformation function; and
wherein the performing the packet digest logging function comprises:
forwarding, by the packet security gateway, the each of the one or more packets corresponding to the packet identification criteria toward its respective destination.
13. The method of claim 1, wherein the packet transformation function comprises an deny packet transformation function; and
wherein the performing the packet digest logging function comprises:
dropping, by the packet security gateway, the each of the one or more packets corresponding to the packet identification criteria.

14. A system comprising at least one processor and a memory storing instructions that, when executed by the at least one processor, cause the system to perform one or more of the methods of claims 1 to 13.

15. A computer program comprising computer-executable instructions that, when executed by one or more processors, cause the one or more processors to perform one or more of the methods of claim 1-13.



European Patent Office
80298 MUNICH
GERMANY
Tel: +49 89 2399 0
Fax: +49 89 2399 4465



Derry, Paul Stefan
Venner Shipley LLP
200 Aldersgate
London EC1A 4HD
ROYAUME-UNI

Formalities Officer
Name: Barrio Baranano, A
Tel: +49 89 2399 - 8621
or call
+31 (0)70 340 45 00

Substantive Examiner
Name: Frank, Mario
Tel: +49 89 2399 - 0

Application No. 15 722 292.8 - 1218	Ref. PSD/81546EP1	Date 16.03.2018
Applicant Centripetal Networks Inc.		

Communication pursuant to Rule 164(2)(b) and Article 94(3) EPC

The examination of the above-identified application has revealed that it does not meet the requirements of the European Patent Convention for the reasons enclosed herewith. If the deficiencies indicated are not rectified the application may be refused pursuant to Article 97(2) EPC.

You are invited to file your observations and insofar as the deficiencies are such as to be rectifiable, to correct the indicated deficiencies within a period

of 6 months

from the notification of this communication, this period being computed in accordance with Rules 126(2) and 131(2) and (4) EPC. One set of amendments to the description, claims and drawings is to be filed within the said period on separate sheets (R. 50(1) EPC).

In accordance with Rule 164(2)(b) EPC you may comment on the search results annexed to this communication and amend the description, claims and drawings of your own volition.

If filing amendments, you must identify them and indicate the basis for them in the application as filed. Failure to meet either requirement may lead to a communication from the Examining Division requesting that you correct this deficiency (R. 137(4) EPC).

Failure to comply with this invitation in due time will result in the application being deemed to be withdrawn (Art. 94(4) EPC).

Registered letter

EPO Form 2001G 11.14TRI



Frank, Mario
Primary Examiner
For the Examining Division

Enclosure(s): 3 page/s reasons (Form 2906)
 EPO Form 2003 - Search results under Rule 164(2)b) EPC

Datum		Blatt		Anmelde-Nr:	
Date	16.03.2018	Sheet	1	Application No:	15 722 292.8
Date		Feuille		Demande n°:	

The examination is being carried out on the **following application documents**

Description, Pages

1-34 as published

Claims, Numbers

1-15 filed in electronic form on 19-06-2017

Drawings, Sheets

1/13-13/13 as published

1 Reference is made to the following documents; the numbering will be adhered to in the rest of the procedure.

D1 US 2004/123220 A1 (JOHNSON ERIK J [US] ET AL) 24 June 2004 (2004-06-24)

D2 US 7 814 546 B1 (STRAYER WILLIAM TIMOTHY [US] ET AL) 12 October 2010 (2010-10-12)

2 The following documents have been cited in the international search report; the numbering will be adhered to in the rest of the procedure.

D3 US 2006/136987 A1 (OKUDA MASATO [JP]) 22 June 2006 (2006-06-22)

D4 US 2007/240208 A1 (YU MING-CHE [TW] ET AL) 11 October 2007 (2007-10-11)

D5 US 2006/146879 A1 (ANTHIAS TEFCROS [US] ET AL) 6 July 2006 (2006-07-06)

D6 US 8 306 994 B2 (KENWORTHY STACY [US]) 6 November 2012 (2012-11-06)

- 3 The following documents have been cited by the applicant in the description; the numbering will be adhered to in the rest of the procedure.
- D7 US 2006/195896 A1 31 August 2006 (2006-08-31)
- D8 US 2006/248580 A1 (FULP) 2 November 2006 (2006-11-02)
- D9 US 2011/055916 A1 (AHN) 3 March 2011 (2011-03-03)
- 4 The present application does not meet the requirements of Article 52(1) EPC because the subject-matter of claim 1 does not involve an inventive step within the meaning of Article 56 EPC.
- 4.1 D1 is considered to be the prior art closest to the subject-matter of claim 1 and discloses (D1 referred to in parentheses) a **method, comprising: receiving, by each of a plurality of packet security gateways** ([0022] "framer logic may be implemented in a variety of ways ... framer may be integrated into a variety of network devices such as routers, switches, firewalls, line cards, network interface cards (NICs), or storage area network (SAN) components, among others") ~~associated with a security policy management server and from the security policy management server,~~ (D1 is not addressing where the policy comes from) **a dynamic security policy that includes at least one rule specifying packet-identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria** ([0009] "framer includes logic that extracts packets from identified frames and generates digests of the packets"); **receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;** ([0003] "a device physically receives signals over a network connection, determines bit values corresponding to the signals, and passes the bits to a framer" This device is part of a protected network, see [0008] "perform packet classification to tailor subsequent processing of a packet. For example, based on packet characteristics, a packet may be given a particular quality of service (QoS), handled with a particular set of security features, or forwarded to a particular destination") **identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria;** ([0009] "framer includes logic that extracts

packets from identified frames and generates digests of the packets") and

performing, by the packet security gateway and on a packet-by-packet basis, the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria. ([0009] "In addition to generating a digest, the framer may also include logic that computes a hash of the digest. A hashing operation can translate the digest into a smaller piece of data that can speed classification table lookups". Thereby, the digest is logged in a particular memory, see [0021] "digest can likely reside in faster access memory than the packet itself")

- 4.2 The subject-matter of claim 1 therefore differs from this known method in that the policy is received from a security policy management server associated with the packet security gateways.
- 4.3 The problem to be solved by the present invention may therefore be regarded as how to deploy the security policy in the packet security gateways.
- 4.4 The solution proposed in claim 1 of the present application cannot be considered to involve an inventive step (Articles 52(1) and 56 EPC) for the following reason. The packet security gateway in D1 (the "framer") is part of network devices (see above cited par [0022]). Therefore, in order to deploy the security policy on these devices the skilled person would use this network without thereby exercising any inventive skill. The server that is inherently used to send the policy to the framer is associated with the framer via this sending step. Accordingly, merely by using the network to deploy the policy, the skilled person arrives at the claimed subject-matter.
- 4.5 Correspondingly, the same objection applies to independent claims 14 and 15.
- 5 Dependent claims 2-13 do not appear to contain any additional features which, in combination with the features of any claim to which they refer, meet the requirements of the EPC with respect to inventive step.